

Network Protection Codes: Providing Self-healing in Autonomic Networks Using Network Coding

Salah A. Aly and Ahmed E. Kamal
 Department of Electrical and Computer Engineering
 Iowa State University, Ames, IA 50011, USA
 Emails: {salah,kamal}@iastate.edu

Abstract—Agile recovery from link failures in autonomic communication networks is essential to increase robustness, accessibility, and reliability of data transmission. However, this must be done with the least amount of protection resources, while using simple management plane functionality. Recently, network coding has been proposed as a solution to provide agile and cost efficient network self-healing against link failures, in a manner that does not require data rerouting, packet retransmission, or failure localization, hence leading to simple control and management planes. To achieve this, separate paths have to be provisioned to carry encoded packets, hence requiring either the addition of extra links, or reserving some of the resources for this purpose.

In this paper we introduce autonomic self-healing strategies for autonomic networks in order to protect against link failures. The strategies are based on network coding and reduced capacity, which is a technique that we call *network protection codes* (NPC). In these strategies, an autonomic network is able to provide self-healing from various network failures affecting network operation. The techniques improve service and enhance reliability of autonomic communication.

Network protection codes are extended to provide self-healing from multiple link failures in autonomic networks. Although this leads to reducing the network capacity, the network capacity reduction is asymptotically small in most cases of practical interest. We provide implementation aspects of the proposed strategies. We present bounds and *network protection code* constructions. Furthermore tables of the best known self-healing codes are presented. Finally, we study the construction of such codes over the binary field. The paper also develops an Integer Linear Program formulation to evaluate the cost of provisioning connections using the proposed strategies, and uses results from this formulation to show that it is more resource efficient from 1+1 protection.

Index Terms—Autonomic networks; network protection codes, self-healing, link failures, network coding, channel coding, and code constructions.

I. INTRODUCTION

Today's communication networks are becoming complex to the degree that the management of such networks has become a major task of network operation. Therefore, the use of network autonomy such that the management functionality and its complexity, is moved to within the network has become the preferred approach, hence giving rise to what is known as autonomic networks [19]. Autonomic networks are self-managed, and they are efficient, resilient, evolvable,

through self-protection, self-organizations, self-configurations, self-healing and self-optimizations (see for example [8], [10], [21] and the references therein). Therefore an autonomic network promotes the autonomy of operational networks with minimum human involvements. However, it is also important not to overload the management plane of autonomic networks to the degree that the management functionality consumes significant amount of computing and communication resources. This paper addresses the self-functionality in autonomic networks, and introduces a technique to provide self-healing that results in simplifying the management plane, as well as the control plane. The technique uses reduced capacities and network coding.

Network coding is a powerful tool that has been used to increase the throughput, capacity, and performance of communication networks [20], [23]. It offers benefits in terms of energy efficiency, additional security, and reduced delay. Network coding allows the intermediate nodes not only to forward packets using network scheduling algorithms, but also encode/decode them using algebraic primitive operations (see [1], [7], [20], [23] and references therein).

One application of network coding that has been proposed recently is to provide network protection against link failures in overlay networks [12], [15]. This is achieved by transmitting combinations of data units from multiple connections on a backup path in a manner that enables each receiver node to recover a copy of the data transmitted on the working path in case the working path fails. This can result in recovery from failures without data rerouting, hence achieving agile protection. Moreover, the sharing of network protection resources between multiple connections through the transmission of linear combinations of data units results in efficient use of protection resources. This, however, requires the establishment of extra paths over which the combined data units are transmitted. Such paths may require the addition of links to the network under the Separate Capacity Provisioning strategy (SCP), or that paths be provisioned using existing links if using the Joint Capacity Provisioning strategy (JCP), hence reducing the network traffic carrying capacity.

Certain networks can allow extra transmissions and the addition of bandwidth, but they do not allow the addition of new transmission lines. In this scenario, one needs to design efficient data recovery schemes. In this paper, we propose such an approach in which we use network coding to provide agile, and resource efficient protection against link failures,

and without adding extra paths. The approach is based on combining data units from a number of sources, and then transmitting the encoded data units using a small fraction of the bandwidth allocated to the connections, hence disposing of the requirement of having extra paths. In this scenario, once a path fails, the receiver can recover the lost packets easily from the neighbors by initiating simple queries.

Previous solutions in network survivability approaches using network coding focused on providing backup paths to recover the data affected by the failures [12]–[14]. Such approaches include 1+N, and M+N protections. In 1+N protection, an extra secondary path is used to carry combinations of data units from N different connections, and is therefore used to protect N primary paths from any single link failure. The M+N is an extension of 1+N protection where M extra secondary paths are needed to protect multiple link failures.

In this paper, we introduce autonomic self-healing and healing-protection network strategies based on network coding and reduced capacity. In these strategies, an autonomic network is able to provide self-healing from various network failures. The techniques improve services and enhance reliability of autonomic communication. We define the concept of *network protection codes* similar to error-correcting codes that are widely used in channel coding [9], [16]. Such codes aim to provide better provisioning and data recovery mechanisms [2].

The new contributions in this paper are stated as follows:

- i) We introduce a self-healing strategy using network coding and a reduced capacity strategy instead of using dedicated paths.
- ii) We provide a new scheme to protect against a single link failure in autonomic networks. The scheme is extended to protect against multiple link failures.
- iii) We develop a theoretical foundation of *protection codes*, in which the receivers are able to recover data sent over t failed links out of n primary links.
- iv) The developed protection strategies are achieved over the binary field, hence the encoding and decoding operations are done using XOR operation.

This paper is organized as follows. In Section II we briefly state the related work and previous solutions to the network protection problem against link failures. In Section III we present the network model and problem definition. Sections IV and V discuss single and multiple link failures and how to protect these link failures using reduced capacity and network coding. In Section VI we give analysis of the general case of $t \ll n$ link failures. Sections VII and VIII present code constructions and bounds on the *network protection code* parameters. In Section IX we present an integer linear program to find the optimal provisioning under the proposed scheme. Section X introduces some numerical results based on the ILP and a comparison between 1+1 protection and the proposed scheme. The paper is concluded in Section XI.

Notations: We fix the notation throughout the paper. Let n , k , m , and t be the number of total connections, working paths, protection paths, and failures, respectively, where $n = k + m$ and $t \leq k$. Let L_i be a connection from a sender s_i to a

receiver r_i . Let c_i be the unit capacity of the connection L_i if it carries plain data (data without coding). \mathbf{F}_2 is a finite field with two elements $\{0, 1\}$. An $[n, k, d_{\min}]_2$ is a *network protection code* defined over \mathbf{F}_2 that has n connections, k working paths, $n - k = m$ protection paths, and recovers from $t = d_{\min} - 1$ failures, where d_{\min} is the minimum distance of the code.

II. RELATED WORK

In this section we will state the related work in network protection strategies against link failures, and linear codes that are used for erasure channels. We define the concept of *network protection codes* similar to error-correcting codes that are widely used in erasure channel coding [9], [16].

A. Revolution Networks Using Network Coding

Network coding is a powerful tool that has been used to increase the throughput, capacity, and performance of communication networks [20], [23]. Network coding assumes that the network nodes not only can forward incoming messages/packets, but also can encode, decode them. It offers benefits in terms of energy efficiency, additional security, and reduced delay (see [1], [7], [20], [23] and references therein). Practical aspects of network coding have been investigated in [6], and bounds on the network coding capacity are investigated in [3], [18].

B. Protection against Failures Using Network Coding

In [12], the author introduced a 1+N protection model in optical mesh networks using network coding over p-cycles. The author suggested a model for protecting N connections from a set of sources to a set of receivers in a network with n connections, where only one connection might fail. Hence, the suggested model can protect against a single link failure in any arbitrary path connecting a source and destination. In [13], the author extended the previous model to protect against multiple link failures. It is shown that protecting against m failures, at least m p-cycles are needed. The idea was to derive m linearly independent equations to recover the data sent from m sources. In [14], the author extended the protection model in [12] and provided a GMPLS-based implementation of a link protection strategy that is a hybrid of 1+N and 1:N. It is claimed that the hybrid 1+N link protection provides protection at higher layers and with a speed that is comparable to the speed achieved by the physical layer implementations. In addition, it has less cost and much flexibility.

In this paper, we provide a new technique for protecting a network against failures using *protection codes* and *reduced capacity*, and for the network to recover from such failures in an agile manner. The benefits of our approach are that:

- i) It allows receivers to recover the lost data without data rerouting, data retransmission or failure localization, hence simplifying the control and management planes.
- ii) It has reasonable computational complexity and does not require adding extra paths or reserving backup paths.
- iii) At any point in time, all n connection paths have full capacity except at one path in case of protecting against

a single link failure and $m < n$ paths in case of protecting against $t \leq m$ link failures.

- iv) The working and protection paths capacities are distributed among each other for fairness.

III. NETWORK MODEL

Let $\mathcal{G} = (V, E)$ be a graph which represents the network topology. V is a set of network nodes and E is a set of edges. Let there be n unidirectional connections, and let $S \subset V$ be the set of sources $\{s_1, \dots, s_n\}$ and $R \subset V \setminus S$ be the set of receiver nodes $\{r_1, \dots, r_n\}$ of the n connections in \mathcal{G} . The case of $S \cap R \neq \emptyset$ can be easily incorporated in our model. Two nodes u and v in V are connected by an edge (u, v) in E if there is a direct connection between them. We assume that the sources are independent of each other, meaning they can only send messages and there is no correlation between them. For simplicity, we will assume that a path exists between s_i and r_i , and it is disjoint from the path between s_j and r_j , for $j \neq i$.

The network model \mathcal{N} can be described in the following assumptions.

- i) Let \mathcal{N} be a network with a set of sources $S = \{s_1, s_2, \dots, s_n\}$ and a set of receivers $R = \{r_1, r_2, \dots, r_n\}$, where $S \cup R \subset V$.
- ii) Let L be a set of links L_1, L_2, \dots, L_n such that there is a link L_i if and only if there is a connection path between the sender s_i and receiver r_i , i.e., L_i corresponds to the path

$$\{(s_i, w_{1i}), (w_{1i}, w_{2i}), \dots, (w_{(\lambda)i}, r_i)\}, \quad (1)$$

where $1 \leq i \leq n$ and $(w_{(j-1)i}, w_{ji}) \in E$, for some integer $\lambda \geq 1$. Hence we have $|S| = |R| = |L| = n$. The n connection paths are pairwise link disjoint.

- iii) Every source s_ℓ sends a packet with its own ID_{s_ℓ} and data x_ℓ to the receiver r_ℓ , so

$$packet_{s_\ell} = (ID_{s_\ell}, x_\ell, \delta), \quad (2)$$

where δ is the round number of the source packet $packet_{s_\ell}$.

- iv) All packets belonging to the same round are sent in the same round slot. The senders will exchange the rule of sending plain and encoded data for fairness, as will be illustrated below.
- v) All links carry uni-directional data from sources to receivers.
- vi) We consider the scenario where the cost of adding a new path is higher than just combining messages in an existing path, or there is not enough resources to provision dedicated paths in the network.

We can define the unit capacity c_i of a link L_i as follows.

Definition 1: The unit capacity of a connecting path L_i between s_i and r_i is defined by

$$c_i = \begin{cases} 1, & L_i \text{ is an active working path;} \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

What we mean by an *active* path is that the receiver is able to receive and process unencoded signals/packets throughout this

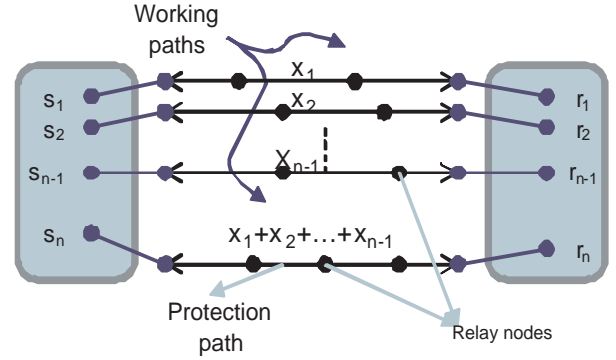


Fig. 1. Network protection against a single path failure using reduced capacity and network coding. One path out of n primary paths carries encoded data. The black points represent various other relay nodes

path. Hence, the protection path is assumed to be inactive. The total capacity of \mathcal{N} is given by the summation of all active path capacities, divided by the number of paths.

This means that each source s_i can send a maximum of one packet per unit time on a link L_i . Assume that all links have the same capacity. One can also always assume that a source with a large rate can be divided into a set of sources, each of which has a unit link capacity.

The following definition describes the *working* and *protection* paths between two network switches as shown in Fig. (1).

Definition 2: The *working paths* in a network with n connection paths carry traffic under normal operations. The data on these paths are sent without encoding. The *Protection paths* in our proposed scheme carry encoded data from other sources. A protection scheme ensures that data sent from the sources will reach the receivers in case of failure on the working paths.

Our goal is to provide an agile and resource efficient self-healing method for n connections without adding extra paths. Unencoded data is sent over a path L_i without adding extra paths, but by possibly reducing the source rates slightly. Linear combinations of data units are sent on these paths alternately, and by using the reduction in working path capacities. The linear combinations are used to recover from failures.

Clearly, if all paths are active then the total capacity of all connections is n .

In general, the total normalized capacity of the network for the active and failed paths is computed by

$$C_{\mathcal{N}} = \frac{1}{n} \sum_{i=1}^n c_i. \quad (4)$$

IV. PROTECTING NETWORKS AGAINST A SINGLE LINK FAILURE

In this section we study the problem of protecting a set of connections against a single link failure in a network \mathcal{N} with a set of sources S and a set of receivers R . This problem has been studied in [12], [13] by provisioning a path that is link disjoint from all connection paths, and passes through all sources and destinations. All source packets are encoded in one

single packet and transmitted over this path. The encoding is dynamic in the sense that packets are added and removed at each source and destination.

Assume that every source s_i has its own message x_i . Also, source s_j forms the encoded data y_j which is defined by

$$y_j = x_1 \oplus \dots \oplus x_{i \neq j} \oplus \dots \oplus x_n \quad (5)$$

where the sum is over the finite field $\mathbf{F}_2 = \{0, 1\}$. In this case, the symbol \oplus is the XOR operation.

Source s_i , for $i \neq j$, sends a packet to the receivers r_i , which is given by

$$\text{packet}_{s_i} = (ID_{s_i}, x_i, \delta). \quad (6)$$

On the other hand,

source s_j sends a packet that will carry the encoded data y_j to the receiver r_j over the link L_j ,

$$\text{packet}_{s_j} = (ID_{s_j}, y_j, \delta). \quad (7)$$

Now we consider the case where there is a single failure on link L_k . Therefore, we have two cases:

- i) If $k = j$, the link L_j has a failure, and the receiver r_j does not need to query any other node since link L_j carries encoded data that is only used for protection. All other receiver nodes receive their data correctly on links which have not failed.
- ii) If $k \neq j$, then the receiver r_k needs to query the other $(n - 1)$ nodes in order to recover the lost data x_k over the failed link L_k . The reason is that x_k exists either at r_j , and it requires information of all other receivers. x_k can be recovered by adding all other $n - 1$ data units. The recovery is implemented by adding y_j and all x_i for $i \neq j$, and $i \neq k$. This follows from Equation (5).

This shows that only one single receiver needs to perform $(n - 2)$ addition operations in order to recover its data if its link fails. In other words, all other receivers will receive the transmitted data from the senders of their own connections with a constant operation $O(1)$.

The following example illustrates the plain and encoded data transmitted from five senders to five receivers.

Example 3: Let S and R be two sets of senders and receivers, respectively, in the network model \mathcal{N} . The following scheme explains the plain and encoded data sent in five consecutive rounds from the five senders to the five receivers.

cycle	1					2	3
rounds	1	2	3	4	5
$s_1 \rightarrow r_1$	y_1	x_1^1	x_1^2	x_1^3	x_1^4
$s_2 \rightarrow r_2$	x_2^1	y_2	x_2^2	x_2^3	x_2^4
$s_3 \rightarrow r_3$	x_3^1	x_3^2	y_3	x_3^3	x_3^4
$s_4 \rightarrow r_4$	x_4^1	x_4^2	x_4^3	y_4	x_4^4
$s_5 \rightarrow r_5$	x_5^1	x_5^2	x_5^3	x_5^4	y_5

The encoded data y_j , for $1 \leq j \leq 5$, is sent as

$$y_j = \sum_{i=1}^{j-1} x_i^{j-1} + \sum_{i=j+1}^5 x_i^j. \quad (8)$$

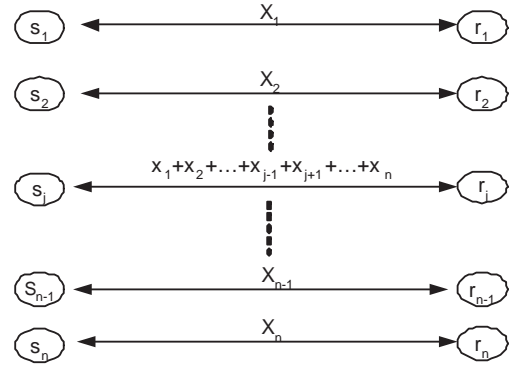


Fig. 2. Network protection against a single link failure using reduced capacity and network coding. One connection out of n primary working paths carries encoded data, i.e. protection path. There are $n - 1$ active working paths carry plain data.

We notice that every message has its own round. Hence the protection data is distributed among all paths for fairness.

A. Network Protection Codes (NPC) for a Single Link Failure

We can define the set of sources that will send encoded packets by using constraint matrices. We assume that there is a *network protection code* $\mathcal{C} \subseteq \mathbf{F}_2^n$ defined by the constraint matrix

$$G = \begin{bmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 \end{bmatrix}_{(n-1) \times n} \quad (10)$$

Without loss of generality, in Matrix (10), for $1 \leq j \leq n-1$, the column vector $(g_{1j} \ g_{2j} \ \dots \ g_{(n-1)j})^T$ in \mathbf{F}_2^{n-1} corresponds to $(n-1)$ sources, say for example the sources s_1, s_2, \dots, s_{n-1} , that will send (update) their values to $(n-1)$ receivers, say i.e., r_1, r_2, \dots, r_{n-1} . Also, there exists one source that will send encoded data, e. g., source n in the above matrix. The row vector $(g_{i1} \ g_{i2} \ \dots \ g_{in})$ in \mathbf{F}_2^n determines the channels L_1, L_2, \dots, L_n .

The weight of a row in G is the number of nonzero elements. We define d_{min} to be the minimum weight of a row in G . Put differently

$$d_{min} = \min\{|g_{ij} \neq 0, 1 \leq j \leq n, 1 \leq i \leq n-1\} \quad (11)$$

Hence, since every row in G has weight of two, $d_{min} = 2$.

We can now define the *network protection code* that will protect a single path failure as follows:

Definition 4: An $[n, n-1, 2]$ *network protection code* \mathcal{C} is a $n-1$ -dimensional subspace of the space \mathbf{F}_2^n defined by the generator systematic matrix G and is able to recover from a single network failure of an arbitrary path L_i .

This means that an $[n, n-1, 2]$ code over \mathbf{F}_2 is a code that encodes $(n-1)$ symbols into n symbols and detects (recovers from) a single path failure. We note that the *network protection*

codes NPC are also error correcting codes that can be used for erasure channels. The positions of errors (failures) are known.

Remark 5: The number of failures that can be recovered by an NPC is equal to the minimum distance of the code minus one, i.e., $t = d_{min} - 1$. Sometimes we refer to NPC by the number of failures t , otherwise they are defined by the minimum distance d_{min} as shown in Table (III).

In general we will assume that the code \mathcal{C} defined by the generator matrix G is known for every source s_i and every receiver r_i . This means that every receiver will be able to recover the data x_i if the link L_i fails, provided that L_i is active in the sense defined in Definition (1). Hence, the rows of the generator matrix G are the basis for the code \mathcal{C} . We assume that the positions of the failures are known. Furthermore, every source node has a copy of the code \mathcal{C} . Without loss of generality, the protection systematic matrix among all sources is given by:

$$\begin{array}{c|ccccc} & L_1 & L_2 & \cdots & L_{n-1} & L_n \\ \hline s_1 & x_1 & 0 & \cdots & 0 & x_1 \\ s_2 & 0 & x_2 & \cdots & 0 & x_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ s_{n-1} & 0 & 0 & \cdots & x_{n-1} & x_{n-1} \\ \hline total & x_1 & x_2 & \cdots & x_{n-1} & y_n \end{array} \quad (12)$$

where y_n is the protection value collected from every source s_i that will be encoded at source s_n , for all $1 \leq i \leq n-1$. Put differently, we have

$$y_n = \sum_{i=1}^{n-1} x_i \quad (13)$$

where the summation operation is defined by the XOR operation.

In a general scenario, the system operates in cycles, where each cycle consists of n rounds, such that at round $1 \leq j \leq n$ of a cycle we have

$$y_j = \sum_{i=1, i \neq j}^n x_i \quad (14)$$

where the round number of a packet x_i is not shown for simplicity with the understanding that it is the first packet in the source's output queue. We assume that every source s_i has a buffer that stores its value x_i and can also send the protection value y_j . Hence in the channel L_j , s_j prepares a packet $packet_{s_j}$ that contains the value

$$packet_{s_j} = (ID_{s_j}, y_j, \delta), \quad (15)$$

and sender s_i for $i \neq j$ will send its data x_i in a $packet_{s_i}$ over the channel L_i defined as follows

$$packet_{s_i} = (ID_{s_i}, x_i, \delta), \quad (16)$$

In general each source will send $(n-1)$ packets containing plain data, and exactly one packet contain encoded data in all n rounds. The transmission will be repeated in cycles, hence every cycle has n rounds.

Recovery from a single path failure is summarized by the next two lemmas.

Lemma 6: Encoding the data from sources $S \setminus \{s_j\}$ at a source s_j in the network \mathcal{N} is enough to protect against a single path failure.

Lemma 7: The total number of encoding operations needed to recover from a single link failure in a network \mathcal{N} with n sources is given by $(n-2)$ and the total number of transmissions is n .

The previous lemma guarantees the recovery from a single arbitrary link failure.

Lemma 8: In the network model \mathcal{N} , through out each cycle, the average network capacity of protecting against a single link failure using reduced capacity and network coding is given by $(n-1)/n$.

Proof: i) We know that every source s_i that sends the data x_i over a working path L_i has capacity $c_i = 1$. ii) Also, the source s_j sends the encoded data y_j at different slots, has an inactive capacity. iii) The source s_j is not fixed among all nodes S , however, it is rotated periodically over all sources for fairness. On average one source of the n nodes will reduce its capacity. This shows the capacity of \mathcal{N} as stated. ■

V. PROTECTING NETWORKS AGAINST MULTIPLE LINK FAILURES

In the previous section we introduced a strategy for self-healing from single link failure for autonomic networks.

However, it was shown in [17] through an experimental study that about %30 of the failures of the Sprint backbone network are multiple link failures. Hence, one needs to design a general strategy against multiple link failures for the purpose of self-healing.

In this section we will generalize the above strategy to protect against t path failures using *network protection codes* (NPC) and the reduced capacity. We have the following assumptions about the channel model:

- i) We assume that any t arbitrary paths may fail and they may or may not be correlated.
- ii) Locations of the failures are known, but they are arbitrary among n connections.
- iii) In order to protect n working paths, k connection must carry plain data, and $m = n - k$ connections must carry encoded data.
- iv) We do not add extra protection paths, and every source node is able to encode the incoming packets independently.
- v) We consider the encoding and decoding operations are performed over \mathbf{F}_2 .

In Sections VIII and VII we will show the connection between error correcting codes that are used for erasure channels and the proposed *network protection codes* [9], [16].

Assume that the notations in the previous sections hold. Let us assume a network model \mathcal{N} with $t > 1$ path failures. One can define a *protection code* \mathcal{C} which protects n links as shown in the systematic matrix G in (17). In general, the systematic matrix G defines the source nodes that will

send encoded messages and source nodes that will send only plain message without encoding. In order to protect n working paths, k connection must carry plain data, and $m = n - k$ connections must carry encoded data.

The generator matrix of the NPC for multiple link failures is given by:

$$G = \left[\begin{array}{ccc|ccc} 1 & 0 & \dots & 0 & p_{11} & \dots & p_{1m} \\ 0 & 1 & \dots & 0 & p_{21} & \dots & p_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & p_{k1} & \dots & p_{km} \end{array} \right], \quad (17)$$

identity matrix $k \times k$ Submatrix $P_{k \times m}$

where $p_{ij} \in \mathbf{F}_2$

The matrix G can be rewritten as

$$G = \left[I_k \mid \mathbf{P} \right], \quad (18)$$

where \mathbf{P} is the sub-matrix that defines the redundant data $\sum_{i=1}^k p_{ij}$ to be sent to a set of sources for the purpose of self-healing from link failures. Based on the above matrix, every source s_i sends its own message x_i to the receiver r_i via the link L_i . In addition m links out of the n links will carry encoded data. Let d_{min} be the minimum distance (minimum weight) of a nonzero vector in the matrix G .

Definition 9: An $[n, k, d_{min}]_2$ network protection code \mathcal{C} is a k -dimensional subspace of the space \mathbf{F}_2^n that is able to recover from all network failures up to $t = d_{min} - 1$.

In general the network protection code (NPC), which protects against multiple path failures, can be defined by a generator matrix G known for every sender and receiver. Also, there exists a parity check matrix H corresponds to G such that $GH^T = 0$. We will restrict ourselves in this work for NPC that are generated by a given generator matrix G in the systematic. In addition, we will assume that the protection codes are defined by systematic matrices defined over \mathbf{F}_2 [9], [16]. An $[n, k, t]_2$ NPC code is also an $[n, k, d_{min}]_2$, where $t = d_{min} - 1$.

Without loss of generality, at one particular round and cycle, the protection matrix (scheme) among all sources is given by

	L_1	L_2	\dots	L_k	L_{k+1}	L_{k+2}	\dots	L_n
s_1	x_1	0	\dots	0	$p_{11}x_1$	$p_{12}x_1$	\dots	$p_{1m}x_1$
s_2	0	x_2	\dots	0	$p_{21}x_2$	$p_{22}x_2$	\dots	$p_{2m}x_2$
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	\vdots	\vdots	\vdots
s_k	0	0	\dots	x_k	$p_{k1}x_k$	$p_{k2}x_k$	\dots	$p_{km}x_k$
T	x_1	x_2	\dots	x_k	y_1	y_2	\dots	y_m

(19)

We ensure that $k = n - m$ paths L_1, L_2, \dots, L_k have full capacity and they carry the plain data x_1, x_2, \dots, x_k . Also, all other m paths have inactive capacity, in which they carry the encoded data y_1, y_2, \dots, y_m . In addition, the m links are not fixed, and they are chosen alternatively between the n connections.

A. Encoding and Recovery Operations

We shall illustrate how the encoding and recovery operations are achieved at the sources and receivers, respectively.

Encoding Process. The network encoding process at the set of senders are performed in a similar manner as in Section IV. Every source s_i has a copy of the systematic matrix G and it will prepare a packet along with its ID in two different cases. First, if the source s_i will send only its own data x_i with a full link capacity, then

$$packet_{s_i} = (ID_{s_i}, x_i, \delta). \quad (20)$$

Second, if \mathbb{S} is the set of sources sending encoded messages, then

$$packet_{s_j} = (ID_{s_j}, \sum_{\ell=1, s_\ell \notin \mathbb{S}}^k p_{\ell j} x_\ell, \delta), \quad (21)$$

where $p_{\ell j} \in \mathbf{F}_2$.

The transmissions are sent in rounds. Therefore, the senders will alternate the role of sending plain and encoded data for fairness.

Recovery Process. The recovery process is done as follows. Assume t failures occur, then a system of linearly independent equations of t variables (corresponding to the data lost due to the failed paths) can be solved. The $packet_{s_i}$ arrives at a receiver r_i with an associated round number, δ . The receiver r_i at time slot n will detect the signal in the link L_i . If the link L_i fails, then r_i will send a query to other receivers in $R \setminus \{r_i\}$ asking for their received data. Assume there are t path failures. Then we have three cases:

- 1) All t link failures have occurred in links that carry encoded packets, i.e., $packet_{s_j} = (ID_{s_j}, \sum_{\ell=1, s_\ell \notin \mathbb{S}}^k p_{\ell j} x_\ell, \delta)$. In this case no recovery operations are needed.
- 2) All t link failures have occurred in links that do not carry encoded packets, i.e., $packet_{s_i} = (ID_{s_i}, x_i, \delta)$. In this case, one receiver that carries encoded packets, e.g., r_j , can send $n - m - 1$ queries to the other receivers with active links asking for their received data. After this process, the receiver r_j is able to decode all messages and will send individual messages to all receivers with link failures to pass their correct data.
- 3) All t link failures have occurred in arbitrary links. This case is a combination of the previous two cases and the recovery process is done in a similar way. Only the lost data on the working paths need to be recovered.

The proposed network protection scheme using distributed capacity and coding is able to recover up to $t \leq d_{min} - 1$ link failures (as defined in Definition (9)) among n paths and it has the following advantages:

- i) $k = n - m$ links have full capacity and their sender nodes have the same transmission rate.
- ii) The m links that carry encoded data are dynamic (distributed) among all n links. So, no single link L_i will always suffer from reduced capacity.

- iii) The encoding process is simple once every sender s_i knows the NPC.
- iv) The recovery from link failures is done in a dynamic and simple way. Only one receiver node needs to perform the decoding process and it passes the data to other receivers that have link failures.

VI. CAPACITY ANALYSIS

We shall provide theoretical analysis regarding our *network protection codes*. One can easily compute the number of paths needed to carry encoded messages to protect against t link failures, and compute the average network capacity. The main idea behind NPC is to simplify the encoding operations at the sources and the recovery operations at the receivers. The following lemma demonstrates the average normalized capacity of the proposed network model \mathcal{N} where r failures occur.

Lemma 10: Let \mathcal{C} be a *network protection code* with parameters $[n, n-m, d_{\min}]$ over \mathbf{F}_2 . Let n and m be the number of sources (receivers) and number of connections carrying encoded packets, respectively, the average normalized capacity of the network \mathcal{N} is given by

$$(n-m)/n. \quad (22)$$

Proof: At one particular round, we have m protection paths that carry encoded data. Hence there are $n-m$ working paths that carry plain data. The result is a direct consequence by applying the normalized capacity definition. ■

Remark 11: In the network protection model \mathcal{N} , in order to protect t network disjoint link failures, the minimum distance d_{\min} of the protection code must be at least $t+1$.

The previous remark ensures that the maximum number of failures that can be recovered is $d_{\min} - 1$, where d_{\min} is the minimum distance of the *network protection code*. For simplicity, we denote a NPC defined over \mathbf{F}_2 by $[n, n-m, d_{\min}]_2$ unless stated otherwise.

For example one can use the Hamming codes with parameters $[2^r - 1, 2^r - r - 1, 3]_2$ to recover from two failures. One can also puncture or extend these codes to reach the required length, i.e., number of connection, see [9] for deriving new codes from known codes by puncturing, extending, shortening those codes. $[7, 4, 3]_2$, $[15, 11, 3]_2$, and $[63, 57, 3]_2$ are examples of Hamming codes that protect against two link failures. The protection code $[15, 11, 3]$ has 15 connections among them are 11 working paths and 4 protection paths, in addition the minimum distance is 3 and the code protects 2 link failures.

Another example is the BCH codes with arbitrary design distance, i.e., $[n, k, d_{\min} \geq \delta]_2$. It is well known that the minimum distance of a BCH code is greater than or equal to its designed distance. References $[15, 11, 3]_2$, $[31, 26, 3]_2$ and $[63, 56, 3]_2$ are examples of BCH codes that protect up to two link failures. Also, $[15, 8, 5]_2$, $[31, 21, 5]_2$ and $[48, 36, 5]_2$ are examples of BCH codes against four link failures [9], [16]. In the next section we will include tables of the best known *network protection codes*.

VII. CODE CONSTRUCTIONS AND BOUNDS

Assume we have n established connections in the network model \mathcal{N} . The goal is to design a good *protection code* that protects t failures. What we mean by a good *protection code* is that for given number of connections n and failures t , it has large number of working paths. Hence the protection code has a high performance. In addition, we establish bounds on the *network protection code* parameters in the next section.

One way to achieve our goal is to design codes with arbitrary minimum distances. The reader can consult any introductory coding theory book, for example [9], [16]. In this case a BCH code with designed distance d and length n can be used to deploy this goal.

We shall quickly review the essential construction of non-primitive narrow-sense BCH codes that will be used in the next section. Let q be a prime power, and n, μ and d be positive integers such that $\gcd(q, n) = 1$, and $2 \leq d \leq n$. Furthermore, μ is the multiplicative order of q modulo n . Let α be a primitive element in \mathbf{F}_{q^μ} . A nonprimitive narrow-sense BCH code \mathcal{C} of designed distance d and length $q^{[\mu/2]} < n \leq q^\mu - 1$ over \mathbf{F}_q is a cyclic code with a generator monic polynomial $g(x)$ that has $\alpha, \alpha^2, \dots, \alpha^{d-1}$ as zeros,

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i). \quad (23)$$

Thus, c is a codeword in \mathcal{C} if and only if $c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{d-1}) = 0$. The parity check matrix of this code can be defined as

$$H_{bch} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \dots & \alpha^{(d-1)(n-1)} \end{bmatrix}. \quad (24)$$

If the minimum distance of this code is $d_{\min} \geq d$, then the code can recover up to $d_{\min} - 1$ failures. In this case the number of connections that will carry plain data is given by:

$$k \leq n - \mu \lceil (d-1)(1-1/q) \rceil. \quad (25)$$

But this is an upper bound in the dimension of the NPC, aka, the number of working connections that carry plain data. Therefore, we seek a result to determine the exact dimension. Fortunately, this can be obtained when the designed distance of BCH codes are bounded. The following Theorem enables one to determine the dimension in closed form for BCH code of small designed distance.

Theorem 12: Let q be a prime power and $\gcd(n, q) = 1$, with $q^\mu \equiv 1 \pmod{n}$. Then a narrow-sense BCH code of length $q^{[\mu/2]} < n \leq q^\mu - 1$ over \mathbf{F}_q with designed distance d in the range $2 \leq d \leq d_{\max} = \min\{\lfloor nq^{[\mu/2]} / (q^\mu - 1) \rfloor, n\}$, has dimension of

$$k = n - \mu \lceil (d-1)(1-1/q) \rceil. \quad (26)$$

Proof: See [4, Theorem 10]. ■

For small designed distance d we can exactly compute the minimum distance of the BCH code, see Tables (I), (II), and (III). Consequently, determine the dimension of the protection code. This helps us to compute the number of failures

TABLE I

BEST KNOWN *network protection codes* AGAINST SINGLE AND DOUBLE LINK FAILURES

n	m	code	type
7	3	$[7, 4, 3]_2$	Hamming code
10	4	$[10, 6, 3]_2$	Linear code
15	4	$[15, 11, 3]_2$	Hamming code
19	7	$[19, 12, 3]_2$	Extension construction
23	8	$[23, 15, 3]_2$	Extension construction
25	5	$[25, 20, 3]_2$	Linear code
31	5	$[31, 26, 3]_2$	Hamming code
39	8	$[39, 31, 3]_2$	Extension construction
47	9	$[47, 38, 3]_2$	Extension construction
63	6	$[63, 57, 3]_2$	Hamming code
71	8	$[71, 63, 3]_2$	Matrix construction
79	9	$[79, 70, 3]_2$	Extension construction
95	10	$[95, 85, 3]_2$	Extension construction
127	7	$[127, 120, 3]_2$	Hamming code

that the *network protection code* can recover. In practical cases, the number of failures t is small in comparison to the number of connections n that makes it easy to exactly compute the parameters of the *network protection codes*. Theorem (12) made it explicit straightforward to derive the exact parameters of NPC based on BCH codes.

We shall give many families of NPC codes derived from BCH codes over \mathbf{F}_2 . One final thing is that one can also start by a code for a given length n , and will be able to puncture, shorten, or extend this code, see [9, Chapter 1.]. This will dramatically change the number of working and protection paths and failures which the code can recover.

A. Bounds on the Code Parameters

Bounds on the code parameters are needed to measure its performance and error recovery and detection capabilities. For a given code parameters length n and dimension k , we establish a bound on the minimum distance of the *protection codes* derived in the previous section.

The most well-known upper bounds on error-correcting codes over symmetric and erasure channels are the Singleton and Hamming bounds [9], [16]. The Singleton bound establishes the relationship between the length, dimension, and minimum distance of the code parameters, i.e. n , k , and d_{min} . However, it does not specify the connection between code parameters and the alphabets size q . The packing bound, known as Hamming bound, takes in consideration the codes parameters n, k, d_{min} along with q .

We can also state upper bounds on the *network protection codes* [9], [16]. The Singleton bound on the *network protection code* parameters are stated as follows. Let t be the number of failure that the code can protect.

$$t \leq n - k \quad (27)$$

The equality in this bound will hold if the size of the used finite field is greater than $n - t$.

One can also state the Hamming bound in the network code

TABLE II

BEST KNOWN *network protection codes* AGAINST UP TO FOUR LINK FAILURES. SUCH CODES CAN BE PUNCTURED, EXTENDED, OR SHORTENED TO OBTAIN THE REQUIRED LENGTH AS SHOWN IN SECTION VIII.

n	m	code	type
15	7	$[15, 8, 5]_2$	Hamming code
19	8	$[19, 11, 5]_2$	Lengthening Hamming-Preparata code
20	11	$[20, 9, 5]_2$	Lengthening Hamming-Preparata code
23	9	$[23, 14, 5]_2$	Linear code
31	10	$[31, 21, 5]_2$	BCH code
33	10	$[33, 23, 5]_2$	Linear code
35	13	$[35, 22, 5]_2$	Shorting Preparata code
63	11	$[63, 52, 5]_2$	Preparata code
70	12	$[70, 58, 5]_2$	Lengthening Hamming-Preparata code
81	13	$[81, 68, 5]_2$	Linear code
128	14	$[128, 114, 5]_2$	BCH code
135	18	$[135, 117, 5]_2$	Shorting Preparata code

parameters as follows.

$$\sum_{i=0}^{\lfloor (d_{min}-1)/2 \rfloor} \binom{n}{i} (q-1)^i \leq q^{n-k} \quad (28)$$

For the binary Hamming bound of m protection paths

$$\sum_{i=0}^{\lfloor t/2 \rfloor} \binom{n}{i} \leq 2^m \quad (29)$$

We have the following lemma on the minimum number of protection paths of *network protection code* parameters.

Lemma 13:

$$m \geq \max \left\{ d_{min} - 1, \log_q \left(\sum_{i=0}^{\lfloor t/2 \rfloor} \binom{n}{i} (q-1)^i \right) \right\} \quad (30)$$

Proof: The proof is a direct consequence from the Singleton and Hamming bounds. Applying Equations (27) and (28) gives the result. ■

VIII. TABLES OF BEST KNOWN PROTECTION CODES

In this section we investigate which codes are suitable for network self-healing against link failures. We will present several *network protection codes* with given generator matrices and exact parameters. The proposed codes are not necessarily optimal, i.e. they do not saturate the Singleton bound. The classical Singleton bound is given by

$$k \leq n - d_{min} + 1 \quad (31)$$

This bound shows that the number of protection paths must be at least $d_{min} - 1$, i.e., $m \geq d_{min} - 1$. The equality of this inequality occurs in case of a single path failure.

We notice that all senders do not participate in the encoding vectors. This means that the proposed codes are suitable for the general protection case where a set of working paths is protected by a protection path. This will reduce our proposed codes to be also used for network protection using p-cycle [12], [14].

The codes shown in Table (I) are used to protect against single and double link failures using their symmetric generator

TABLE III
FAMILIES OF BCH CODES THAT CAN BE USED AS *network protection codes*
AGAINST LINK FAILURES.

n	m	BCH Code
15	4	[15, 11, 3]
15	7	[15, 8, 4]
15	8	[15, 7, 5]
31	5	[31, 26, 3]
31	5	[31, 26, 3]
31	10	[31, 21, 5]
31	15	[31, 16, 7]
31	10	[31, 11, 11]
31	25	[31, 6, 15]
127	14	[127, 113, 5]
127	49	[127, 78, 15]
127	21	[127, 106, 7]
127	50	[127, 77, 27]

matrices. Also, the codes in Table (II). Table (III) presents the best known BCH codes for arbitrary minimum distance over \mathbf{F}_2 .

Given a NPC with parameters $[n, k, d_{min}]$, one can possibly obtain a new NPC by shortening, extending, or puncturing this code. If there is an NPC \mathcal{C} with parameters $[n, k, d_{min}]_2$, then by i) shortening \mathcal{C} yields a code with parameters $[n - 1, k - 1, d_{min}]_2$, ii) puncturing \mathcal{C} yields a code with parameters $[n - 1, k, d_{min} - 1]_2$, iii) appending \mathcal{C} yields a code with parameters $[n + 1, k, d_{min} + 1]_2$, iv) extending \mathcal{C} yields a code with parameters $[n + 1, k + 1, d_{min}]_2$.

For example, if there is a BCH Hamming code with parameters $[15, 11, 3]_2$, then there must be codes with parameters $[14, 10, 3]_2$ (by shortening), $[14, 11, 2]_2$ (by puncturing), $[16, 11, 4]_2$ (by appending), $[16, 12, 3]_2$ (by extending). The interested readers might consult textbooks in classical coding theory for further propagation rules [9], [16].

A. Illustrative Examples

Example 14: Consider a BCH code \mathcal{C} with parameters $[15, 11, 3]_2$ that has designed distance 3 and generator matrix G given by:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (32)$$

The code \mathcal{C} over \mathbf{F}_2 can be used to recover from two link failures since its minimum distance is 3. One can puncture, shorten, or extend this code to obtain the required code length, which determines the total number of disjoint connections. In this example we have 15 connections, and 11 primary working paths. Furthermore, the links $L_{12}, L_{13}, L_{14}, L_{15}$ will

carry encoded data. The matrix G presents the construction of NPC, and the senders that will send encoded and plain data.

Example 15: The code \mathcal{C} has parameters $[15, 8, 4]_2$ and generator matrix G given by:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (33)$$

This means that all senders s_1, \dots, s_8 will send plain data over the working connection L_1, \dots, L_8 . Also, the senders s_9, \dots, s_{15} will send encoded data over the protection paths L_9, \dots, L_{15} . In this encoding scheme, the connection L_9 will carry encoded data from s_1, s_5, s_7 and s_8 .

IX. ILP FORMULATION

The problem of finding link disjoint paths between pairs of nodes in a graph is known to be an NP-complete problem [22]. Hence, even finding the working paths in this problem is hard. We therefore introduce an Integer Linear Program (ILP) for solving the reduced capacity network coding-based protection problem introduced in this paper.

The purpose of the ILP is to find a feasible provisioning for groups of connections, such that:

- The paths used by a group of connections protected together are mutually link disjoint.
- There is a circuit, \mathbf{S} , which connects the sources of all connections protected together, and this circuit is link disjoint from the working paths. The \mathbf{S} circuit is used to exchange source data units in order to form the linear combination of data units to be sent on the path used for that purpose.
- There is a circuit, \mathbf{R} , which connects the receivers of all connections protected together, and this circuit is link disjoint from the working paths. The \mathbf{R} circuit is used by the receivers to recover from lost data units due to a failure.
- The total number of links used by the working paths, the \mathbf{S} circuit and the \mathbf{R} circuit is minimal.

We assume that the number of channels per span is not upper bounded, i.e., the network is uncapacitated.

The following table defines the input parameters to the ILP:

N	number of connections
s_h	source of connection h
r_h	destination of connection h
δ^{hl}	a binary indicator which is equal to 1 if connections h and l have the same destination
γ^{hl}	a binary indicator which is equal to 1 if connections h and l have the same source

The variables used in the formulation are given below:

- n^{hl} binary variable which is 1 if and only if connections h and l are protected together
- z_{ij}^h binary variable which is 1 if and only if connection h uses link (i, j) on the working path
- p_{ij}^h binary variable which is 1 if and only if connection h uses link (i, j) on its **S** circuit
- q_{ij}^h binary variable which is 1 if and only if connection h uses link (i, j) on its **R** circuit
- $b_{i,j}^h$ binary variable which is 1 if connection h uses link (i, j) on its backup path
- P_j^{hl} binary variable, which is 1 if and only if the **S** circuits for connections h and l share a node, j (required if $n^{hl} = 1$).
- Q_j^{hl} binary variable, which is 1 if and only if the **R** circuits for connections h and l share a node, j (required if $n^{hl} = 1$ and $\delta^{hl} = 0$).
- P^h binary variable, which is 1 if and only if connection h is protected with another connection that has a source different than that of h (this variable is important since if h is not protected with another such connection, there is no need for the **S** circuit).
- Q^h binary variable, which is 1 if and only if connection h is protected with another connection that has a destination different than that of h (this variable is also important since if h is not protected with another such connection, there is no need for the **R** circuit).
- \mathcal{P}_{ij}^{hl} binary variable which is 1 if and only if connections h and l are protected together, and share link (i, j) on the **S** circuit.
- \mathcal{Q}_{ij}^{hl} binary variable which is 1 if and only if connections h and l are protected together, and share link (i, j) on the **R** circuit.
- $\pi_{i,j}^h$ binary variable which is equal to 1 if connection h is the lowest numbered connection, among a number of jointly protected connections, to use link (i, j) on its **S** circuit (used in computing the cost of the **S** circuit).
- $\theta_{i,j}^h$ binary variable which is equal to 1 if connection h is the lowest numbered connection, among a number of jointly protected connections, to use link (i, j) on its **R** circuit (used in computing the cost of the **R** circuit).
- $\beta_{i,j}^h$ binary variable which is equal to 1 if the secondary protection path for connection j uses link (i, j) .

Minimize:

$$\sum_{i,j,h} (z_{i,j}^h + \beta_{i,j}^h + 0.5\pi_{i,j}^h + 0.5\theta_{i,j}^h)$$

In the above, the summation is the cost of the links used by the connections' working paths and the **S** and **R** circuits. It also includes the cost of a secondary circuit for 1+1 protection, in case network coding-based protection cannot be used. The calculation of these cost factors will be explained using the constraints below.

Subject to:

The following constraints are enforced in the working and protection paths.

I- Constraints on working paths:

$$z_{i,s_h}^h = 0 \quad \forall h, i \neq s_h \quad (34)$$

$$z_{r_h,j}^h = 0 \quad \forall h, j \neq r_h \quad (35)$$

$$\sum_{i \neq s_h} z_{s_h,i}^h = 1 \quad \forall h \quad (36)$$

$$\sum_{i \neq r_h} z_{i,r_h}^h = 1 \quad \forall h \quad (37)$$

$$\sum_i z_{ij}^h = \sum_i z_{ji}^h \quad \forall h, j \neq s_h, r_h \quad (38)$$

$$z_{ij}^h + z_{ji}^h + z_{ij}^l + z_{ji}^l + n^{hl} \leq 2 \quad \forall h, l, i, j \quad (39)$$

Equations (34), (36), (35) and (37) ensure that the traffic on the working path is generated and consumed by the source and destination nodes, respectively. Equation (38) guarantees flow continuity on the working path. Equation (39) ensures that the working paths of two connections which are protected together are link disjoint. Since a working path cannot use two links in opposite directions on the same span (or edge in the graph), then two connections which are protected together cannot use the same span either in the same, or opposite directions. Such a condition is included in Equation (39).

II- Constraints on secondary protection circuits:

$$b_{i,s_h}^h = 0 \quad \forall h, i \neq s_h \quad (40)$$

$$b_{r_h,j}^h = 0 \quad \forall h, j \neq r_h \quad (41)$$

$$\sum_{i \neq s_h} b_{s_h,i}^h = 1 \quad \forall h \quad (42)$$

$$\sum_{i \neq r_h} b_{i,r_h}^h = 1 \quad \forall h \quad (43)$$

$$\sum_i b_{ij}^h = \sum_i b_{ji}^h \quad \forall h, j \neq s_h, r_h \quad (44)$$

$$\beta_{ij}^h \geq b_{ij}^h - \sum_l n^{hl} \quad \forall h, l, i, j \quad (45)$$

$$\beta_{ij}^h + z_{ij}^h \leq 1 \quad \forall h, i, j \quad (46)$$

The above constraints evaluate the cost of the secondary protection paths used for 1+1 protection. There are two sets of variables in the calculation of this cost. The first one is the b_{ij}^h variables, which are evaluated in Equations (40)-(44) using exactly the same way the z_{ij}^h variables are evaluated. However, the cost that goes into the objective function depends on whether connection h is protected with another connection using network coding or not. The variables which evaluate this cost are the β_{ij}^h variables, and are evaluated in Equation (45), which makes it equal to b_{ij}^h only if the connection is not protected with another connection. Finally, Equation (46) makes sure that the working and the used secondary paths are link disjoint.

III- Constraints on P circuits:

$$P^h \geq n^{hl} - \gamma^{hl} \quad \forall h, l \quad (47)$$

$$\sum_i p_{s_h i}^h = P^h \quad \forall h, i \neq s_h \quad (48)$$

$$\sum_i p_{i s_h}^h = P^h \quad \forall h, i \neq s_h \quad (49)$$

$$\sum_i p_{ij}^h = \sum_i p_{ji}^h \quad \forall h, j \quad (50)$$

$$z_{ij}^h + \frac{p_{ij}^h + p_{ji}^h}{2} \leq 1 \quad \forall h, i, j \quad (51)$$

$$z_{ij}^h + \frac{p_{ij}^l + p_{ji}^l}{2} + n^{hl} \leq 2 \quad \forall h, i, j \quad (52)$$

$$\sum_i (p_{ij}^h + p_{ji}^l) \geq 2P_j^{hl} \quad \forall h, l, j \quad (53)$$

$$\sum_i (p_{ji}^h + p_{ij}^l) \geq 2P_j^{hl} \quad \forall h, l, j \quad (54)$$

$$\sum_j P_j^{hl} \geq n^{hl} - \gamma^{hl} \quad \forall h, l \quad (55)$$

Equation (47) ensures that the source of connection, h will be connected to a **S** circuit only if it is jointly protected with another connection, l . However, there is one exception to this case, which is the case in which the two connections h and l have the same source. In this case, the **S** circuit is not needed, and this is why γ^{hl} is subtracted from the right hand side of the equation. Notice that if h is protected together with another connection that has a different source, then Equation (47) will then require that a **S** circuit be used. Equations (48) and (49) will ensure that traffic leaves and enters s_h using the **S** circuit, only if it is jointly protected with another connection that has a different source, i.e., when $P^h = 1$. Equation (50) guarantees connection h 's flow continuity on the **S** circuit. Equation (51) makes sure that the working path and its **S** circuit are link disjoint, while Equation (52) makes sure that if two connections h and l are jointly protected, then the **S** circuit of l must also be disjoint from the working path of connection h . Notice that both of Equations (51) and (52) allow a **S** circuit to use two links in opposite directions on the same span, and this is why the sum of the corresponding link usage variables is divided by 2 in both equations. Equations (53), (54) and (55) make sure that if two connections, h and l , are protected together ($n^{hl} = 1$), then their **S** circuits must have at least one joint node ($P_j^{hl} = 1$ for some j). However, similar to Equation (47), a **S** circuit is not needed if the two connections have the same source, hence the subtraction of γ^{hl} from the right hand side of Equation (55).

Notice that in the ILP formulation, the constraints implement the **S** circuit as a set of paths, such that there is a path from each source back to itself. However, the requirement of at least one joint node between every pair of such paths as enforced by constraint (55) will make sure that the **S** circuit takes the form of a tree.

IV- Constraints on R circuits:

$$Q^h \geq n^{hl} - \delta^{hl} \quad \forall h, l \quad (56)$$

$$\sum_i q_{r_h i}^h = Q^h \quad \forall h, i \neq r_h \quad (57)$$

$$\sum_i q_{i r_h}^h = Q^h \quad \forall h, i \neq r_h \quad (58)$$

$$\sum_i q_{ij}^h = \sum_i q_{ji}^h \quad \forall h, j \quad (59)$$

$$z_{ij}^h + \frac{q_{ij}^h + q_{ji}^h}{2} \leq 1 \quad \forall h, i, j \quad (60)$$

$$z_{ij}^h + \frac{q_{ij}^l + q_{ji}^l}{2} + n^{hl} \leq 2 \quad \forall h, i, j \quad (61)$$

$$\sum_i (q_{ij}^h + q_{ij}^l) \geq 2Q_j^{hl} \quad \forall h, l, j \quad (62)$$

$$\sum_i (q_{ji}^h + q_{ji}^l) \geq 2Q_j^{hl} \quad \forall h, l, j \quad (63)$$

$$\sum_j Q_j^{hl} \geq n^{hl} - \delta^{hl} \quad \forall h, l \quad (64)$$

Equations (56)-(64) are similar to Equations (47)-(55), but they apply to the destinations and to the **R** circuit. Therefore, the variables P^h , γ^{hl} , p_{ij}^h and P_j^{hl} are replaced by Q^h , δ^{hl} , q_{ij}^h and Q_j^{hl} , respectively.

Constraints on joint protection:

$$n^{hl} + n^{lm} - 1 \leq n^{hm} \quad \forall h, l, m \quad (65)$$

Equation (65) makes sure that if connections h and l are protected together, and connections l and m are also protected together, then connections h and m are protected together.

V- Constraints for cost evaluation:

$$\mathcal{P}_{ij}^{hl} \leq \frac{p_{ij}^h + p_{ji}^l + n^{hl}}{3} \quad \forall i, j, h, l \quad (66)$$

$$\mathcal{Q}_{ij}^{hl} \leq \frac{q_{ij}^h + q_{ji}^l + n^{hl}}{3} \quad \forall i, j, h, l \quad (67)$$

$$\pi_{ij}^l \geq p_{ij}^l - \sum_{h=1}^{l-1} \mathcal{P}_{ij}^{hl} \quad \forall l, i, j \quad (68)$$

$$\theta_{ij}^l \geq q_{ij}^l - \sum_{h=1}^{l-1} \mathcal{Q}_{ij}^{hl} \quad \forall l, i, j \quad (69)$$

Equations (66), (67), (68) and (69) are used to evaluate the cost of the **S** and **R** circuits, which are used in the objective function. Equation (66) will make sure that \mathcal{P}_{ij}^{hl} cannot be 1 unless connections h and l are protected together and share link ij on the **S** circuit. Equation (67) will do the same thing for the **R** circuit. Note that both \mathcal{P}_{ij}^{hl} and \mathcal{Q}_{ij}^{hl} should be as large as possible since this will result in decreasing the cost of the **S** and **R** circuits, as shown in Equations (68) and (69). In equation (68), π_{ij}^l for connection l will be equal to 1 only if it is not protected on link ij with another lower indexed connection, and will be equal to 0 otherwise. That is, it is the lowest numbered connection among a group of jointly protected connections that will contribute to the cost of the links shared by the **S** circuit. θ_{ij}^l , which is evaluated by Equation (69) will also follow a similar rule, but for the **R** circuit.

TABLE IV
COST COMPARISON BETWEEN 1+1 AND 1+N PROTECTION FOR
NETWORKS WITH $|V| = 6$, $|E| = 9$; $|V| = 8$, $|E| = 12$; AND
 $|V| = 10$, $|E| = 20$.

$ V , E $	N	1+1			NPC		
		Total	Working	Spare	Total	Working	Spare
6, 9	4	15	6	9	14	6	8
	5	17	6	11	12	6	6
8, 12	4	19	9	10	16	8	8
	6	26	10	16	21	11	10
10,20	4	16	6	10	12	6	6
	6	23	10	13	19	9	10

X. ILP EVALUATION AND COST COMPARISON

In this section results from the ILP formulation developed in the previous section to evaluate the cost of provisioning circuits to provide self-healing in autonomic networks using the proposed *network protection codes*. The ILP was solved using the Cplex linear programming solver [11]. We also compare the cost of provisioning NPC to that of provisioning 1+1 protection. The cost of 1+1 protection is evaluated using Bhandari's algorithm [5].

We ran the ILP for various network topologies. The network topologies are generated randomly. First, we consider a bidirectional network with 6 nodes and 9 edges along with 4 and 5 connections. Second, we consider a network with 8 nodes and 12 edges along with 4 and 6 connections. Finally, we consider a network with 10 nodes and 20 edges, while provisioning 4 and 6 connections.

The results shown in Table (IV) indicate that the cost of provisioning self-healing using NPC is always lower than that using 1+1 protection, and the saving in the protection resources can reach up to 30%. For example, consider a network with 8 nodes, 12, and 6 connections. The total cost of using the 1+1 strategy is 26, while the total cost of using NPC is 21. The total saving in resources in this case is close to 20%. However, the saving in the protection resources only is more than 30%. The advantage of using NPC over 1+1 protection may even improve further with the size of the network. For example, for the case of the network with 10 nodes, 20 edges, and 4 connections, the total cost of 1+1 protection is 16, while the total cost of NPC is 12, which means a total saving of 25%. The saving in the protection resources is also 40% in this case.

XI. CONCLUSIONS

We studied a model for recovering from network link failures using network coding. We defined the concept of *network protection codes* to protect against a single link failure, and then extended this concept and the techniques to protect against t link failures using network coding and reduced capacity. Such *protection codes* provide self-healing in autonomic networks with a reduced control and management plane complexity. We showed that the encoding and decoding processes are simple and can be done in a dynamic way. We also developed an ILP formulation to optimally provision communication sessions and the circuits needed to implement NPC. This formulation was then used to assess the cost of

implementing this strategy, and to compare it to the cost of using 1+1 protection. It was shown that the use of NPC for self-healing has an advantage over 1+1 protection, in terms of the cost of connection and backup circuit provisioning.

REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. Inform. Theory*, 46:1204–1216, 2000.
- [2] S. A. Aly and A. E. Kamal. Network protection codes against link failures using network coding. In *Proc. IEEE GlobelComm '08, New Orleans, LA*, December 1-4 2008. arXiv:0809.1258v1 [cs.IT].
- [3] S. A. Aly, V. Kapoor, J. Meng, and A. Klappenecker. Bounds on the network coding capacity for wireless random networks. In *Third Workshop on Network Coding, Theory, and Applications, NetCod'07*, January 2007. arXiv:0710.5340v1 [cs.IT].
- [4] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007. arXiv:quant-ph/0604102v1.
- [5] R. Bhandari. *Survivable Networks: Algorithms for Diverse Routing*. Springer, 1999.
- [6] P. A. Chou, Y. Wu, and K. Jain. Practical network coding. *41st Allerton Conf. Comm., Ctrl. and Comp.*, Monticello, IL, Oct. 2003.
- [7] C. Fragouli, J. Le Boudec, and J. Widmer. Network coding: An instant primer. *ACM SIGCOMM Computer Communication Review*, 36(1):63–68, 2006.
- [8] X. Gu, J. Strassner, J. Xie, L. C. Wolf, and T. Suda. Autonomic multimedia communications: where are we now? *Proc. of IEEE*, 96:1, 2008.
- [9] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.
- [10] IBM. *autonomic computing initiative*. online: <http://www.research.ibm.com/autonomic/manifesto/autonomic-computing.pdf>, 2001.
- [11] ILOG. <http://www.ilog.com>.
- [12] A. E. Kamal. 1+N protection in optical mesh networks using network coding on p-cycles. In *Proc. of the IEEE Globecom*, 2006.
- [13] A. E. Kamal. 1+N protection against multiple faults in mesh networks. In *Proc. of the IEEE International Conference on Communications (ICC)*, 2007.
- [14] A. E. Kamal. Gmpls-based hybrid 1+N link protection over p-cycles: Design and performance. In *Proc. of IEEE Globecom*, 2007.
- [15] A. E. Kamal. A generalized strategy for 1+N protection. In *Proc. of the IEEE International Conference on Communications (ICC)*, 2008.
- [16] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [17] A. Markopoulou, S. Iannaccone, G. Bhattacharyya, C. N. Chuah, and C. Diot. Characterization of failures in an ip backbone network. In *Proc. of IEEE INFOCOM '04*, March 2004.
- [18] A. Ramamoorthy, J. Shi, and R. D. Wesel. On the capacity of network coding for random networks. *IEEE Trans. Info. Theory*, 51(8):2878–2885, Aug. 2005.
- [19] S. Schmid, M. Sifalakis, and D. Hutchiso. Towards autonomic networks. *Lecture Notes in Computer Science*, 4195:1–11, 2006.
- [20] E. Soljanin and C. Fragouli. Network coding information flow perspective. 2007.
- [21] G. Tesaro. Reinforcement learning in autonomic computing. *IEEE Internet comput.*, 11:22–30, 2007.
- [22] J. Vygen. NP-completeness of some edge-disjoint paths problems. *Discrete Appl. Math.*, 61:83–90, 1995.
- [23] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang. *Network Coding Theory*. Now Publishers Inc., 2006.